UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,791	04/02/2004	Marco Macchetti	02AG50553433	9927

27975 7590 06/09/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	**PAPER NUMBER**
2132	

NOTIFICATION DATE	DELIVERY MODE
06/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/816,791	MACCHETTI ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to a Request for Continued Examination filed on April 30, 2008. Claims 12-34 are currently pending.

Response to Arguments

1. Applicant's arguments, see Remarks, filed April 1, 2008, with respect to the rejection(s) of claim(s) 12, 17, 23, and 28 under Coppersmith et al. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Davida et al. [US 4275265].

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 12-14, 16-17, 20-28, and 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davida et al. [US 4275265], hereinafter Davida.

Regarding claim 12, Davida teaches a method for generating output bytes corresponding to respective input bytes [Davida Fig 2] according to a one-to-one binary function [Davida 5: 1-5] representing a cryptographic algorithm [Davida 3: 52], the method comprising: decoding an input byte [Davida 4: 35-43] [Davida 7: 58-61] and generating at least one bit string that contains only one active bit [Davida 4: 38-45]; using an array of logic gates for logically combining bits of the at least one bit string according to the one-to-one binary function [Davida 5: 10-35] [Official notice is taken

that it is common and well known in the art that a decoder circuit can be made out of an array of logic gates for logically combining bits of the at least one bit string from smaller sized decoders known as “decoder expansion."] and generating a 256-bit string [Davida 7: 44-68 –Consider n=8 bits, k=8 bits, which means that a plain text input has 8 bits, and substitution box will operate on one plain text input, decoder would have to generate a 256 bit string.]; and encoding the 256-bit string for obtaining an output byte [Davida 4: 54-68].

Regarding claim 13, Davida teaches a method according to claim 12, wherein the decoding comprises subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the 256-bit string [Official notice is taken that it is common and well known in the art that a decoder circuit can be made out from smaller sized decoders in a technique known as “decoder expansion." Since it is common and well known in that art that a 2-to-4 decoder is an abstraction of 2 1-to-2 decoders and an array of 4 2-input AND gates, it would have been obvious to extend this to an 8-to-256 decoder by having 2 4-to-16 decoders and an array of 256 2-input AND gates.]

Regarding claim 14, Coppersmith et al. teach a method according to claim 12, wherein the input byte is decoded in a corresponding auxiliary 256-bit string [Davida 4: 35-43] [Davida 7: 58-61]; and the 256-bit string is obtained by changing an order of the bits of

the auxiliary 256-bit string according to the one-to-one binary function [Davida 5: 10-35].

Regarding claim 16, Davida teaches a method according to Claim 13, wherein the array of logic gates comprises AND gates, with each bit of the output string is obtained by ANDing among the bits of the subdivided input strings [Official notice is taken that it is common and well known in the art that a decoder circuit can be made out from smaller sized decoders in a technique known as “decoder expansion." Since it is common and well known in that art that a 2-to-4 decoder is an abstraction of 2 1-to-2 decoders and an array of 4 2-input AND gates, it would have been obvious to extend this to an 8-to-256 decoder by having 2 4-to-16 decoders and an array of 256 2-input AND gates.].

Claims 17, 23, and 28 are rejected using the same references as claim 12. Claim 17 is still the same method that uses the same steps as claim 12. Claim 23 and 28 are both apparatus that performs the same method of claim 12.

Claims 20, 24, are rejected using the same references as claim 13. Claim 20 is still the same method that uses the same steps as claim 13. Claims 24 is the apparatus performing the method of claim 13.

Claims 26, 33, are rejected using the same references as claim 24. Claims 26 and 33 are both apparatus having limitations about the digital component devices that would have been inherent in the references anticipating claim 24.

Claims 21, 27, and 34 are rejected using the same references as claim 14. Claims 21 is still the same method that uses the same steps as claim 14. Claims 27 and 34 are both apparatus that performs the same method of claim 14.

Claim 31 is rejected using the same references and rationale as claim 13. Claim 31 is the apparatus performing the same method of claim 13.

Claims 22, 25, and 32 are rejected using the same references and rationale as claim 16. Claim 22 is still the same method performing the method claim 16. Claim 25 and 32 are both apparatus that performing the method of claim 16.

2. Claims 15, 18-19, and 29-30 rejected under 35 U.S.C. 103(a) as being unpatentable over Davida et al. [US 4275265], hereinafter Davida, and further in view of Morioka et al. [IDS Morioka et al, 2002], hereinafter Morioka.

Regarding claim 15, Davida teaches the method according to claim 12.

Davida does not teach wherein the one-to-one binary function represents a ByteSub operation of a Rijndael AES encryption/decryption algorithm.

Morioka teaches optimizing S-box circuits that represent the ByteSub operation of the Rijndael AES encryption/decryption algorithm.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the method of Davida to represent the ByteSub operation as the optimized S-box circuit of the Rijndael AES encryption/decryption algorithm as depicted by Morioka et al. because the method of Davida can be used as a sub-function of the Rijndael AES encryption/decryption algorithm. The suggestion/motivation for combining would have been to optimize the S-box circuit of the Rijndael AES design for low power consumption [Morioka et al., abstract]. Therefore, it would have been obvious to combine Davida and Morioka to obtain the invention as specified in claim 15.

Claims 18-19, and 29-30 are rejected using the same references and rationale as claim 15. Claims 18-19 are still the same method performing the method of claim 15. Claims 29-30 are both apparatus performing the method of claim 15.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Kime et al. "Logic and Computer Design Fundamentals. Chapter 4 –Combinational Functions and Circuits." 2004. Slide 9-11 --Decoder Expansion technique is common and well known in the art for designing decoder circuits.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner. Art Unit 2132.

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132